

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD W. NAGEL
CLERK OF COURT

3/30/31

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3:21MJ124

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WEST. DIV. DAYTONSkype accounts with the user names
live:.cid.58d10c2422ccf850 and live:stphs141963 that is
stored at Microsoft Corporation USA

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-3

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B-3

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

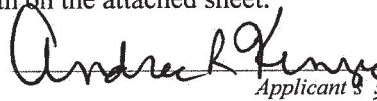
Code Section

SEE ATTACHMENT C-3

Offense Description

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 Applicant's Signature

Andrea R. Kinzig, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone _____ (specify reliable electronic means).Date: 3/30/21City and state: Dayton, OH

Judge's signature

Sharon L. Ovington

Printed name and title

ATTACHMENT A-3

Information associated with the Skype accounts containing the user names of **live:.cid.58d10c2422ccf850** and **live:stphs141963** and/or associated with the telephone number **937-626-4691** or the email address **stphs141963@gmail.com** that is stored at premises controlled by Microsoft Corporation USA, a company that accepts service of legal process at 1 Microsoft Way, Redmond, Washington, 98052.

ATTACHMENT B-3
Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation USA (the “Provider”)

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

1. The contents of all communications associated with the account, including stored or preserved copies of all voicemail messages, audio files, video files, text, text files, images, multimedia, chats, and instant messages (“IMs”) stored and presently contained in, or on behalf of, the account or identifier;
2. Skype Online Records, Skype Out Records, Short Message System (SMS) Records, Skype Wi-Fi Records, and all other transactional information of all account activity, including logs of all incoming and outgoing voice calls and other communications, with the date and time of each communication, the telephone numbers and/or accounts involved each communication, and the Internet Protocol (“IP”) address, Media Access Control (“MAC”) addresses, mobile identifiers, and any other network/device identifiers associated with each communication or other account activity;
3. Registration Details, Billing Address, and all other records or information regarding the identification of the account, including full name, physical address, telephone numbers and other identifiers, the date and time when the account was created, the IP and MAC addresses used to register the account, the length of service, the types of service utilized, records of session times and durations, login IP and MAC addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account numbers);
4. Skype Online Current Subscriber List and all other records or other information stored at any time by an individual using the account, using address books, contact and buddy lists, calendar data, pictures, and files;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;
6. For the account listed in Attachment A-2, all Microsoft accounts that are linked to any of the accounts listed in Attachment A-2 by cookies, creation IP address, recovery email address, and/or telephone number;

7. For the account listed in Attachment A-2, all settings and services used related to chat backups, including the destination (i.e., iCloud or Google Drive);
8. All Neoprints, including the profile contact information; status updates; links to videos, photographs, articles, and other items;
9. Email and Password records.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyn Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and attempted receipt of child pornography), 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession and attempted possession of child pornography), 2251(a) and (e) (production and attempted production of child pornography), 2422(b) (coercion and enticement), and 1470 (transfer of obscene materials to minors), from January 1, 2020 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and production of child pornography; coercion and enticement; and transfer of obscene materials to minors.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, dating websites, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-3

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(2)	Possession and Attempted Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession and Attempted Possession of Child Pornography
18 U.S.C. §2252(a)(2) & (b)(1)	Receipt and Attempted Receipt of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Attempted Receipt of Child Pornography
18 U.S.C. §2251(a) and (e)	Production and Attempted Production of Child Pornography
18 U.S.C. §2422(b)	Coercion and Enticement
18 U.S.C. §1470	Transfer of Obscene Materials to Minors

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the FBI and Department of Homeland Security Investigations, I am currently involved in an investigation of child pornography and child exploitation offenses committed by SEAN T. PORTER (hereinafter referred to as "PORTER"). This Affidavit is submitted in support of Applications for search warrants for the following:
 - a. Information associated with the Google accounts **stphs141963@gmail.com**, **sean2598@gmail.com**, and **portersean68@gmail.com** that is stored at premises controlled by Google LLC (as more fully described in Attachment A-1);
 - b. Information associated with the Meet24, FastMeet, Meet4U, and/or MeetEZ accounts containing the user identification numbers of **45521409**, **45675752**, **45766959**, **45834215**, **45868159**, **45887212**, and **47432599** and/or associated with the email addresses **sean2598@gmail.com** and **portersean68@gmail.com** that is stored at premises controlled by Wildec LLC (as more fully described in Attachment A-2);
 - c. Information associated with Skype accounts containing the user names of **live:.cid.58d10c2422ccf850** and **live:stphs141963** that is stored at premises controlled by Microsoft Corporation USA (as more fully described in Attachment A-3); and
 - d. Information associated with the Snapchat account containing the user name of **sporter4020** (as more fully described in Attachment A-4).
3. The purpose of the Applications is to search for and seize evidence of suspected violations of the following:

- a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography;
 - b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive or attempt to receive child pornography through interstate commerce;
 - c. 18 U.S.C. §§ 2251(a) and (e), which make it a crime to produce or attempt to produce child pornography;
 - d. 18 U.S.C. § 2422(b), which makes it a crime to use a facility of interstate or foreign commerce to coerce and entice of a minor to engage in illegal sexual activities or attempt to do so; and
 - e. 18 U.S.C. § 1470, which makes it a crime to transfer obscene materials to minors.
4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-4 hereto and are incorporated by reference.
 5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
 6. This Affidavit is intended to show that there is sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 through A-4) and does not contain every fact known to the investigation.
 7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(1), 2252(a)(2) and (b)(1), 2252A(a)(2) and (b)(1), 18 U.S.C. §§ 2252(a) and (e), 18 U.S.C. § 2422(b), and 18 U.S.C. § 1470, are present within the information associated with the above noted accounts (as described in Attachments A-1 through A-4).

JURISDICTION

8. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A)

& (c)(1)(A). Specifically, the Court is “a district court of the United States” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. § 2252(a)(2) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
10. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
11. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
12. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
13. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting

interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

14. 18 U.S.C. § 1470 states that it is a violation for any person to knowingly use the mail or any facility or means of interstate or foreign commerce to transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so.
15. 18 U.S.C. § 2422(b) states that is a violation for any person to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or to attempt to do so.
 - a. For purposes of the statute, 18 U.S.C. §2427 states that the term “sexual activity for which any person can be charged with a criminal offense” includes the production of child pornography, as defined in section 2256(8).
16. Ohio Revised Code (O.R.C.) § 2907.04, Unlawful Sexual Conduct with a Minor, states that it is a violation for any person who is 18 years of age or older to engage in sexual conduct with another, who is not the spouse of the offender, when the offender knows that the other person is 13 years of age or older but less than 16 years of age, or if the offender is reckless in that regard.
 - a. O.R.C. § 2907.01 states that the term “sexual conduct” means vaginal intercourse between a male and female; anal intercourse, fellatio, and cunnilingus between persons regardless of sex; and, without privilege to do so, the insertion, however slight, of any part of the body or any instrument, apparatus, or other object into the vaginal or anal opening of another. Penetration, however slight, is sufficient to complete vaginal or anal intercourse.
17. Tennessee Code Annotated § 39-13-506(c), Aggravated Statutory Rape, states that it is a violation for a defendant to sexually penetrate a victim, or for a victim to sexually

penetrate a defendant, when the victim is at least 13 but less than 18 years of age and the defendant is at least 10 years older than the victim.

BACKGROUND INFORMATION

Definitions

18. The following definitions apply to this Affidavit and Attachments B-1 through B-4 to this Affidavit:
- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).
 - e. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the

duration of the session that the client computer is connected to the Internet (or other network).

- f. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- g. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- h. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- i. **“Social Media”** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users’ account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.
- j. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Collectors of Child Pornography

19. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
 - d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors often place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years.
 - e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Google Services

- 20. Google LLC (“Google”) is a multi-national corporation with its headquarters located in Mountain View, California. Google offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.
- 21. In addition, Google offers an operating system (“OS”) for mobile devices (including cellular phones) known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.
- 22. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.
- 23. Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below. Google’s services include but are not limited to the following:
 - a. Gmail: Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google

preserves emails associated with a Google Account indefinitely, unless the user deletes them.

- b. Contacts: Google provides address books for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.
- c. Calendar: Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.
- d. Messaging: Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.
- e. Google Drive: Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive

Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called “Shared with me”. Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

- f. Google Keep: Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google’s cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive.
- g. Google Photos: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.
- h. Google Maps: Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.
- i. Location History: Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may

be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

- j. Chrome and My Activity: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.
 - k. Android Backup: Android device users can use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, call history, contacts, device settings, or SMS messages. Users can also opt-in through Google One to back up photos, videos, and multimedia sent using Messages
24. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

25. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.
26. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.
27. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.
28. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.
29. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.
30. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to

access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

31. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).
32. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.
33. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

Wildec LLC Dating Applications

34. Wildec LLC is a software developer company based in Everett, Washington. Wildec LLC produces a number of dating applications for mobile devices, including Meet24, FastMeet, Meet4U, and MeetEZ.
35. Meet24 is a free dating application available on android cellular telephones, iPhones, and iPod Touches. Similar to other dating applications, Meet24 allows users to create account profiles. Account profiles typically include a profile picture, a profile name, an age, a geographic location, and a statement about the user's status. Individuals can also include other information in their profiles such as their sexual orientation, height, body weight, ethnicity, education, smoking preference, etc.
36. The Meet24 application uses geolocation information to allow users to find dating partners in their geographic areas. The application also allows users to exchange direct text messages, photographs, and video messages with other users.
37. FastMeet, Meet4U, and MeetEZ are other free online dating applications available on android cellular telephones, iPhones, and iPod Touches. These applications provide users with similar features as the Meet24 application, including the ability to exchange direct text messages, photographs, and video messages with other users.

38. Based on my training and experience, I know that individuals frequently change their account profiles on dating applications such as Meet24. Some individuals frequently change their profile pictures, profile names, ages, and physical locations. It is not uncommon for individuals to list inaccurate ages on their profiles. Older individuals sometimes identify themselves as being younger than they actually are in an effort to make themselves appear more attractive to younger potential partners.
39. I have learned that in or around May 2019, the Federal Trade Commission (FTC) issued a warning that three of Wildec LLC's dating applications – that being Meet24, FastMeet, and Meet4U – appeared to violate the Children's Online Privacy Protections Act. Media reports stated that these applications did not prevent users who were under the age of 13 years old from using the applications or being visible to other users. In response to these concerns, both Apple and Google temporarily removed the applications from their respective application stores. The three applications were restored after Wildec LLC updated their terms and conditions for use to state that users under the age of 18 years old could not use their websites.
40. Based on my training and experience, I know that many social media and dating websites (currently to include Meet24, FastMeet, Meet4U, and MeetEZ) state that minors cannot use the websites. Based on my training and experience, I know that Meet24 and other social media and dating websites have little to no means to enforce this policy. I also know, based on my training and experience, that minors commonly utilize these websites. I have been involved in a number of prior investigations in which minors utilized the social media and dating websites that they are supposedly prohibited from using. In these cases, the minors were targeted and sexually exploited by adult offenders.
41. To use the Meet24, FastMeet, Meet4U, and MeetEZ applications, users must complete a registration process that includes providing information such as a profile name, email address, gender, birthday, and location. Wildec LLC maintains this registration information that is provided by its users, as well as other information such as the registration dates and the IP addresses utilized to register the accounts. Wildec LLC assigns its users with unique user identification numbers during the registration process.
42. Wildec LLC maintains various other records and information regarding the use of its accounts. This information includes transactional records such as logs of IP addresses utilized to access the accounts, session dates and times, and the last login dates of the accounts. The information also includes various contents of the accounts, including the following:
 - a. Profile pictures and other information maintained on the account profiles (including information such as the users "status", height, weight, gender, etc.);
 - b. Photos, video messages, voices messages, and other files uploaded by the users and/or exchanged with other users via direct messages;

- c. Contents of direct messages exchanged with other users;
- d. Searches performed by the users;
- e. Information regarding other users that have been added to the user's "Favourites" list;
- f. Records regarding other users that have blocked the user or that the user has blocked; and
- g. Privacy and account settings of its users.

Skype

- 43. Skype owns and operates a communication service that transmits voice calls, video, and messages over the Internet. In May 2011, Skype was acquired by Microsoft Corporation USA, a company based in Redmond, Washington.
- 44. Skype users can make and receive local, long distance, and international phone calls; participate in video chats or send and receive video messages; send and receive short message system (SMS) text messages; and send and receive electronic files including documents, pictures, audio, and video.
- 45. Skype may be installed and used on a desktop computer, laptop, tablet, or mobile phone, including those using operating systems from Apple, Blackberry, Google, and Windows.
- 46. Skype requires users to provide basic contact information to the company during the registration process. This information may include identification data such as name, username, address, telephone number, mobile number, email address, and profile information such as age, gender, country of residence, and language preference.
- 47. Skype users can elect to make public profile information consisting of images, links to personal web pages, and links to social media websites. Skype users may also subscribe to other Skype users with whom they are interested or associated.
- 48. When its users communicate with non-Skype users, the company keeps transaction records during the normal course of business commonly referred to as call detail records. These call detail records consist of the date, time, sender, receiver, duration, and contents of phone calls, text messages, and video messages. According to the company, the transactional records are maintained for six months and data files are stored for 30 to 90 days depending on the type of file.

49. In order to use Skype's premium features like voicemail or to make calls to a landline, cellular telephone, or service outside of the Skype network, a customer must either purchase credits or agree to a monthly or otherwise recurring payment option. This necessitates either providing the company with credit card information, including name, billing address, and credit card number, or the use of an online payment processor such as PayPal.
50. Skype retains system information about the types of devices a customer uses to access their service. This can include computer platform and operating system, Internet Protocol (IP) address information, and mobile device information such as device type, manufacturer name, model number, operating system, and cellular service provider.
51. Skype users may elect to import their contacts from email and social media accounts. This contact information can include name, email address, and/or phone numbers.
52. Skype accesses and stores location information regarding its customers. The location information includes Wi-Fi access points when a customer uses Skype from a home or free Wi-Fi spot, global positioning system (GPS) data when a user searches for free Skype Wi-Fi access points, and GPS data when a Skype user shares their location with another user.
53. Skype users can link their social media accounts with the communication provider. These social media accounts may include Microsoft Corporation, LinkedIn, and Twitter. Skype users may also use an associated Microsoft account and other services. These associated services may include online file storage, Microsoft email services, and/or other Microsoft products or services.
54. Skype also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Skype, including the information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.
55. Skype uses the following terms to describe the data in its possession:
 - a. Registration Details: This includes information captured at the time the account was created. This may include identification data such as name, username, address, telephone number, mobile number, email address, and profile information such as age, gender, country of residence, language preference, and any user profile information.
 - b. Billing Address: The billing address provided by the user that is used in conjunction with payment for Skype services.
 - c. Skype Online Current Subscription List: A list of Skype users currently subscribed to by the user.

- d. Purchase History: Financial transactions with Skype including method of payment information and billing address.
 - e. Skype Out Records: Historical call detail records for calls placed to cellular and landline phone numbers.
 - f. Skype Online Records: Historical call detail records for calls placed to the Skype number from landline and mobile numbers.
 - g. Short Message System Records (SMS): Text messages including the content of the messages.
 - h. Skype Wi-Fi Records: Historical records of connections to Skype Wi-Fi access points.
 - i. Email and Password Records: Historical records of emails and password change activities.
56. Communication providers such as Microsoft Corporation typically retain additional information about their users' accounts during the normal course of business, such as information about the length of service (including start date), the types of services utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Skype users may communicate directly with Skype about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Providers like Microsoft Corporation typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

Snapchat Accounts

57. Snapchat is a social media communication application owned by Snap Inc., a company based in Santa Monica, California. The application is available on cellular telephones and tablets. The application provides a means to send and receive "self-destructing" messages, pictures, and videos.
58. A "snap" is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed, it is deleted from the company's system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaves the Chat screen, messages viewed by both the sender and receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can

send pictures to other users by utilizing the camera on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and “snaps” constitute “electronic communications” within the meaning of 18 U.S.C. § 3123. See 18 U.S.C. §§ 3127(1) and 2510(12).

59. A user can type messages and send photos, videos, audio notes, and video notes to friends within the Snapchat application using the “Chat” feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat application itself, a user can opt to save part of the Chat by tapping on the message that he or she wants to keep. The user can clear the message by tapping it again.
60. “Our Stories” is a collection of user-submitted “Snaps” from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at an event could all contribute to the same “Our Stories” collection by sharing their snaps, even if they do not know each other. Users can also view “Our Stories” events if they are not actually present at the event by subscribing to the story.
61. In addition to “Our Stories”, a Snapchat user can keep a sort of photo / video diary using the “Story” feature. Each snap in a “Story” documents the user’s experience. Based on the user’s privacy settings, the photos and videos added to a “Story” can be viewed either by everyone on Snapchat or just the user’s friend. Stories are visible to other users for up to 24 hours.
62. “Snapcash” is an online money transfer service offered by Snapchat. The actual business platform is run by “SquareUp”, the distributor of a mobile credit card reader and application Square Register. Snapcash can be used to transfer money between Snapchat users using a linked, U.S.-issued Visa or MasterCard debit card only. Snapcash can only be sent to other users who have a linked debit card. Snapcash has a \$250 weekly limit but can be upgraded to a \$2,500 weekly limit. Users who upgrade have to provide their full name, date of birth, and Social Security Number.
63. Snapchat has a “Group Stories” feature that allows multiple users to contribute photos and videos to the same “Story”, a collection of posts that stays viewable for a limited amount of times. Snapchat users can name their group story and invite other users and “friends” by user name to add content. The Group Stories will disappear if 24 hours pass without a user adding a new photo or video.
64. “Memories” is a cloud-storage service provided by Snapchat. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone’s photo gallery in Snapchat’s Memories. A user can also edit and send Snaps and create Stories from

these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.

65. Snapchat asks users to provide basic contact and personal identifying information when registering their accounts, to include date of birth. When a user creates an account, he/she creates a unique Snapchat user name. This is the name visible to other Snapchat users. An email address is required to register a Snapchat account, and a new user must also provide a mobile telephone number. This telephone number is verified during the registration process. Snapchat sends an activation code to the telephone number that must be entered before proceeding with the registration step. However, a user may elect to bypass entering a telephone number, so one may not always be present in the user's account. Snapchat also retains the account creation date.
66. While a Snapchat message may disappear, the record of who sent it and when it was sent still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.
67. Snapchat stores device information such as the model, operating system, operating system version, mobile device telephone number, and mobile network information of devices used in conjunction with the service. Snapchat also collects unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event that the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.
68. If a user consents, Snapchat can access his/her device's electronic phone book or contacts list and images.
69. Snapchat retains information about the method and source of payment of customers who use the Snapcash service. This includes debit card information such as the card number, expiration date, CVV security code, and billing address zip code. Additionally, the company may have the date of birth and Social Security Number of those involved in money transfers. Snapcash generates a receipt for any transactions. The receipts are programmed to automatically delete after the sender and recipient have seen the message and swiped out of the Chat screen, unless either taps to save the message. Snapchat maintains transactional records for ten days. These records include information about the sender and receiver, the transaction amount, and the date/time stamps of when the message was sent, received, and opened.

70. Snapchat deletes a snap once it had been viewed. If the message is not read because the user has not opened up the application, the message is stored for 30 days before being deleted. However, just because the snap no longer appears to the user does not necessarily mean they are gone. For example, Snapchat has a feature called Replay. This allows users to view a previously viewed snap once per day. This feature is disabled by default and the user must opt-in to use Replay. Also, if a Snapchat user posts an image or video to the MyStory feature, it can be viewed by their friends for 24 hours. If the users posts to the Our Stories feature, the snaps are archived and can be viewed through Snapchat.
71. Therefore, the computers of Snap Inc. are likely to contain the material described above, including stored electronic communications and information concerning subscribers and their use of Snapchat (such as account access information, transaction information, and account application).

WhatsApp

72. WhatsApp is a cross-platform centralized messaging and voice-over IP (VOIP) service owned by Facebook Inc. The WhatsApp application allows users to send text messages and voice messages, make voice and video calls, and share files (including images, videos, and documents). The WhatsApp application runs on mobile devices, but it is also accessible from desktop computers as long as the user's mobile device remains connected to the Internet while he/she uses the desktop application.
73. WhatsApp requires that users provide a standard cellular telephone number when registering with the service. The latest version of the application contains end-to-end encryption to secure messages.

FACTS SUPPORTING PROBABLE CAUSE

Criminal History for PORTER

74. Records from the Hamilton County (Ohio) Common Pleas Court revealed that PORTER was convicted on or around April 29, 2003 of one count of Attempted Sexual Conduct with a Minor, in violation of O.R.C. § 2907.04(A), and one count of Soliciting Another by Means of a Telecommunications Device to Engage in Sexual Activity, in violation of O.R.C. § 2907.07(E)(2) (pursuant to case C/03/CRA/9889). PORTER was sentenced to six months of imprisonment.
75. Records from the Greene County (Ohio) Common Pleas Court revealed that PORTER was convicted on or around May 16, 2005 of two counts of Importuning, in violation of O.R.C. § 2907.07(D)(2) (pursuant to case 2004-CR-533). PORTER was sentenced to twelve months of imprisonment.

76. Records from the United States District Court for the Southern District of Ohio revealed that PORTER was convicted in or around January 2009 of one count of Possession of Child Pornography, in violation of 18 U.S.C §§ 2252(a)(4)(B) and (b)(2) (pursuant to case 3:08CR163). PORTER was sentenced to 120 months of imprisonment and lifetime of supervised release.

PORTER's Term of Supervised Release

77. On or around February 28, 2018, PORTER was released from the Bureau of Prisons' custody from his 2009 conviction and began his lifetime term of supervised release. He is currently supervised by Probation Officer (PO) Christopher Owens of the United States Probation Service in Dayton, Ohio. As part of the conditions of his supervised release, PORTER is prohibited from using, owning, or possessing any computer or computer-related equipment without prior approval of his probation officer. PORTER is also required to permit the installation of software to monitor the computer activities on any computer device that he is authorized to use.
78. Based on information from PO Owens, I have learned the following additional information about PORTER:
- a. PORTER resides at 2317 Adrian Court in Dayton, Ohio (hereinafter referred to as the "SUBJECT PREMISES"). PO Owens has conducted regular home visits at this residence and has verified that PORTER resides there. The most recent home visit was conducted on or around March 9, 2021.
 - b. PORTER's brother also previously resided at the SUBJECT PREMISES. During the most recent home visit (on or around March 9, 2021), PORTER reported to PO Owens that the brother had moved out of the SUBJECT PREMISES.
 - c. PO Owens previously provided authorization for PORTER to utilize a flip-style cellular telephone bearing telephone number 937-626-4691 and a Samsung Model SM-T650NU tablet. PO Owens has not authorized PORTER to utilize any other electronic devices.
 - d. PO Owens has communicated with PORTER via telephone number 937-626-4691.
 - e. Monitoring software utilized by the United States Probation Service was installed on PORTER's Samsung tablet on or around April 24, 2019. PO Owens has utilized this monitoring software to periodically review PORTER's activities on the tablet. PO Owens also periodically manually reviewed PORTER's cellular telephone and tablet during home visits. PO Owens has not located any child pornography or unauthorized contents on PORTER's tablet or cellular telephone during these reviews.

- f. PORTER has reported to PO Owens that he (PORTER) utilizes the email address **stphs141963@gmail.com**.
- g. PO Owens has observed PORTER driving a navy blue Ford Explorer. PO Owens has also observed a gray Chevrolet Trailblazer and a motorcycle parked at the SUBJECT PREMISES.

Sex Offender and Ohio Bureau of Motor Vehicles Information

- 79. As part of the three prior convictions detailed above, PORTER is currently required to register as a sex offender. PORTER initially completed his sex offender registration paperwork on or around January 31, 2018. He is required to renew his registration on a semi-annual basis. On his current sex offender registration paperwork, PORTER identified that he resides at the SUBJECT PREMISES and drives two motor vehicles: a 2006 Chevrolet Trailblazer and a 2017 Ford Explorer.
- 80. Records from the Ohio Bureau of Motor Vehicles identified that PORTER utilizes the SUBJECT PREMISES on his current Ohio driver's license. This driver's license was issued on or around March 10, 2018. Records from the Ohio Bureau of Motor Vehicles also identified that a 2006 Chevrolet Trailblazer and a 2017 Ford Explorer are presently registered to PORTER at the SUBJECT PREMISES.

2020 Undercover Investigation by FBI Memphis Division

- 81. In 2020 and 2021, the Memphis division of the FBI conducted various online, covert investigations to identify individuals utilizing dating applications to communicate with and sexually exploit minors. In November 2020, an FBI agent acting in an undercover capacity (hereinafter referred to as "UCO-1") utilized a profile on the Meet24 website posing as a 14-year old female child. UCO-1's account profile picture depicted a clothed female¹. The account profile stated that UCO-1 was an 18-year old female, but her² status stated "Im really 14".
- 82. On or around November 10, 2020, an individual utilizing the profile name of "Mike" contacted UCO-1 via Meet24's direct text messaging feature. UCO-1 viewed the Meet24 account profile for "Mike" and saw that the profile picture depicted a white male. The account profile for the account stated that "Mike" was 20 years old and lived in Moraine, Ohio.

¹ The profile pictures that UCO-1 utilized, as well as other pictures she sent to "Mike" throughout the course of the investigation (as further detailed below), actually depict an adult female who appears young. This adult female consented for the FBI to utilize her photographs as part of online undercover child exploitation investigations.

² Although UCO-1 is a male FBI agent, he will be referred to in this Affidavit with female pronouns given that he was using a female persona.

- a. I have compared the “Mike” profile picture to PORTER’s current Ohio driver’s license photograph. Based on this comparison, it appears that PORTER is depicted in the “Mike” profile picture.
83. “Mike” communicated with UCO-1 via Meet24’s direct text messaging feature during the approximate time period of November 10, 2020 through November 18, 2020. Below is a summary of these communications:
- a. “Mike” inquired about UCO-1’s age, and UCO-1 identified that she was 14 years old. UCO-1 reiterated her age on multiple occasions throughout the communications. “Mike” identified that he was 43 years old.
 - i. PORTER is currently 58 years old. Based on my training and experience, I know that individuals who utilize dating websites often falsely identify their ages. Individuals often portray themselves as being younger than they are as a means to make themselves appear more attractive to younger individuals.
 - ii. Also based on my training and experience, I know that individuals involved in child exploitation offenses often falsely portray their names, ages, and/or the locations where they reside as a means to conceal their identities from law enforcement officers.
 - b. “Mike” inquired on several occasions if UCO-1 was a law enforcement officer. “Mike” also inquired if UCO-1 hid the communications on her cellular telephone from her mother.
 - c. “Mike” inquired about UCO-1’s past sexual experiences and if she liked older men. “Mike” told UCO-1 that he would like to have sex with her. Later in the communications, “Mike” told UCO-1 that he could not meet with her in person because it would be illegal to do so. However, he noted that they could still have “fun” on the Meet24 application.
 - d. “Mike” asked UCO-1 for nude pictures of herself.
 - i. Based on my training and experience, I know that “Mike’s” requests for nude photographs are consistent with individuals who are attempting to coerce and entice minors to produce child pornography, which the offenders are attempting to receive and possess.
 - e. When “Mike” continued to ask UCO-1 for pictures of herself, UCO-1 suggested that he send her pictures depicting other girls who were posing how he wanted her

to pose. "Mike" sent UCO-1 an image of a young female child wearing a bathing suit with her legs spread apart. "Mike" then claimed that he did not know how he got that picture, and that he did not have any "nudes" of young girls (presumably referring of nude photographs of minors).

- f. "Mike" sent two images of his nude genitalia to UCO-1. These images did not include the man's face.
 - i. Based on my training and experience, I believe that these images are obscene.
- g. "Mike" also sent UCO-1 another picture that purportedly depicted himself. This picture included the man's face
 - i. Based on comparing this photograph to PORTER's current Ohio driver's license photograph, it appears that PORTER is the individual depicted in the photograph sent by "Mike" to UCO-1.
- h. Below are excerpts from the Meet24 chats summarized above:

Mike: I'm just horny lol
Mike: how old are you
UCO-1: im 14. u?
UCO-1: ok then sorry
Mike: I'm 43
Mike: do you like older men
UCO-1: yeah i guess. i am tired of boys my age
Mike: can I see a picture of you
UCO-1: *Sends clothed image of a female*
Mike: you look older then 14
Mike: why are you tired of boys
UCO-1: well thanks. im almost 15
UCO-1: have u met 14 year okd boys? they are so stupid and awkward lol
Mike: I was 14 once I understand
Mike: have you had sex yet
Mike: are you there
UCO-1: im a virgin but done other stuff
Mike: what have you done
UCO-1: like made out and given hand jobs and blow jobs and stuff
Mike: do you like that stuff
Mike: have you had pussy ate
UCO-1: nobody ever gone down on me yet
Mike: I would
Mike: where are you from

UCO-1: TN
Mike: how can I be sure you are real and not a cop
UCO-1: im not a cop lol seriously
Mike: you never know
Mike: send me a nude of you to prove it
UCO-1: f off not doing that. scam.
.....
UCO-1: my mom was calling me i talked to her is that ok
Mike: yeah that's okay as long as your mother doesn't bother us
Mike: does she ever check your phone or computer to see if you're
talking with older men
.....
Mike: I wish you were a couple years older kind of scares me to talk to
you it's not really right
UCO-1: y not?
Mike: because you are only 14 years old and I'm 43
Mike: what makes you want an older man besides the young boys being
immature
UCO-1: i dont care bout age but if u do we don't have to talk i understand
Mike: I mean if you just want to have sex why not have it with a young
boy I mean when I was 14 my dick was just as big as it is today
Mike: no we can still talk
.....
[When UCO-1 didn't reply to Mike's messages]:
Mike: are you in your bedroom
Mike: see that makes you seem like a cop just leaving me and I are
probably going to prosecute before what I didn't so s***
UCO-1: stop it
Mike: so why did you stop talking to me
UCO-1: i was busy sorry
UCO-1: ur kinda bossy
.....
UCO-1: shes home [referring to UCO-1's mother]
Mike: does she check your phone or whatever you're using
.....
Mike: how old did you say you were again because you look older than
14
Mike: I'm not saying you're older than 14 I'm just asking
UCO-1: im 14. same as yesterday.
Mike: so when do you turn 15
UCO-1: march
Mike: do you like talking to me
Mike: he really care about my age
UCO-1: i dont care about age

Mike: so have you had sex yet I don't remember if you told me that or not and I can't look back on it because I deleted all my texts

UCO-1: no im a virgin

Mike: so why do you want to talk to older men

.....

Mike: don't get me wrong I think you are very beautiful I wish you were 18 years old right now

UCO-1: look we don't have to talk if u don't want to

Mike: no I want to talk with you I like you

Mike: I'm just kind of nervous you are a cop

Mike: because a lot of cops pose this little girls 14 years old or whatever and they want to bust big guys for talking to

UCO-1: omg

Mike: what do you mean

UCO-1: lets just not talk anymore u seem to not be comfortable with it. sorry.

Mike: no I want to talk with you

.....

Mike: *Sends image of a male who appears to be PORTER*

UCO-1: *Sends two clothed images of a female*

Mike: you look beautiful baby

Mike: did you say you had sex I can't remember I'm sorry I'm a little buzzed tonight

Mike: no you told me you were a virgin

UCO-1: lol. im a virgin

UCO-1: but i done ither stuff

Mike: until you want to have sex

Mike: would you like to have sex with me

UCO-1: yeah maybe

Mike: I would love to have sex with you

UCO-1: yeah lol

Mike: I would love to be with you

UCO-1: ok mite be fun loo

UCO-1: lol

Mike: do you want to see a naked of me

UCO-1: sure if u want me to

Mike: I like that you're open

Mike: *Sends image of a nude male (whose face is not captured in the image) holding an erect penis*

UCO-1: nice

Mike: he like that baby

Mike: do you like that baby

Mike: *Sends close-up image of a male holding his penis*

UCO-1: looks good to me

Mike: I like you baby can you send me a new picture of you

Mike: I want to see a nude
UCO-1: oh i don't have any nude pics
Mike: can't you take a picture
UCO-1: i mean maybe. what u wanna see?
Mike: just stand in front of your camera take your clothes off let me see
your body
UCO-1: i really don't like sending pics like that
Mike: but it's with me baby I will never trade it with anybody else I
promise you that
.....
UCO-1: send me some pics of girls from the internet in poses u want me to
do and then ill take pics in the same pose
Mike: I just want you to be nature
Mike: *Sends image depicting a female child wearing a bathing suit with
her legs spread apart*
Mike: can you do that please
UCO-1: no. cause im not 6 years old lol
Mike: I don't have any nudes of any young girls
Mike: I don't even know where I got that picture at
Mike: let me see wireless looking through my pictures
Mike: I'm just going to let you know okay
Mike: I just want to see you picture I want to see something that shows
me that you're real
.....
Mike: you know I know you're only 14 but you're making me fall in love
with you
UCO-1: lol ok
Mike: so you want to really continue to keep in contact with me
UCO-1: yeah sure
Mike: I would love to keep in contact with you too
Mike: maybe when you're 18 we can get together but I can't do that
before then that would be a legal one he would be wrong
UCO-1: ok
Mike: I'm not discouraging you but I just can't meet somebody that's
under age
Mike: does it mean we can have fun here though

2021 Undercover Investigation by FBI Memphis Division

84. In February 2021, an FBI agent acting in an undercover capacity (hereinafter referred to as “UCO-2”)³ utilized a profile on the Meet24 website posing as a 13-year old female child. UCO-2’s account profile picture depicted a clothed female⁴. The account profile stated that UCO-1 was an 18-year old female, but her status stated “Im 18 minus 5”.
85. On or around February 14, 2021, an individual utilizing the profile name of “Sean” contacted UCO-2 via Meet24’s direct text messaging feature. UCO-2 viewed the Meet24 account profile for “Sean” and saw that the profile picture depicted a white male. The account profile identified that “Sean” was 20 years old and lived in Moraine, Ohio.
- a. I have compared the “Sean” profile picture to PORTER’s current Ohio driver’s license photograph. Based on this comparison, it appears that PORTER is depicted in the “Sean” profile picture.
86. “Sean” communicated with UCO-2 via Meet24’s direct text messaging feature during the approximate time period of February 14, 2021 through February 15, 2021. Below is a summary of these communications:
- a. “Sean” began the communications by telling UCO-2 that he had a sexual relationship with his 12-year old daughter. “Sean” sent UCO-2 a photograph of a female child, which he purported to be of his daughter. When UCO-2 questioned “Sean” about his relationship to this child, he then stated that he did not actually have a daughter.
- i. Based on the investigation conducted to-date, it does not appear that PORTER has a daughter.
- ii. Based on my training and experience, I know that individuals involved in child exploitation offenses sometimes fabricate information about sexual experiences they have had with minors. Such individuals do so, among other reasons, as a means to gauge the victims’ possible interest in having a sexual relationship with an adult, to de-sensitize the victims to sexually explicit conduct, to test the victims, and to express their own sexual fantasies.

3 The same FBI agent who operated the “UCO-1” persona also operated the “UCO-2” persona. Given that a different persona was utilized, this FBI agent will be referred to as “UCO-2” for the 2021 communications. Similar to the 2020 communications, UCO-2 will be referred to in this Affidavit with female pronouns even though the FBI agent is a male.

4 The profile pictures that UCO-2 utilized, as well as other pictures she sent to “Sean” throughout the course of the investigation (as further detailed below), actually depict an adult female who appears young. This adult female consented for the FBI to utilize her photographs as part of online undercover child exploitation investigations.

- b. “Sean” inquired about UCO-2’s age, and UCO-2 identified that she was 13 years old. UCO-2 reiterated her age on multiple occasions throughout the communications. “Sean” identified that he was 47 years old. “Sean” claimed that although his profile stated that he lived in Ohio, he actually lived in Covington, Kentucky.
 - i. PORTER is currently 58 years old. Based on my training and experience, I know that individuals who utilize dating websites often falsely identify their ages. Individuals often portray themselves as being younger than they are as a means to make themselves appear more attractive to younger individuals.
 - ii. Also based on my training and experience, I know that individuals involved in child exploitation offenses often falsely portray their names, ages, and/or the locations where they reside as a means to conceal their identities from law enforcement officers.
- c. “Sean” inquired about UCO-2’s past sexual experiences and if she liked older men. “Sean” talked about the possibility of meeting UCO-2 in person to engage in sexually explicit conduct, and he said that he would like to perform oral sex on her.
- d. “Sean” inquired if UCO-2 thought about older men when she masturbated. “Sean” then said that he thought about girls who were UCO-2’s age when he masturbated, and that talking to her “turns me on”.
- e. “Sean” asked UCO-2 for a picture of her vagina.
 - i. Based on my training and experience, I know that “Sean’s” request for a picture of UCO-2’s vagina is consistent with individuals who are attempting to coerce and entice minors to produce child pornography, which the offenders are attempting to receive and possess.
- f. “Sean” sent an image of a man’s nude genitalia to UCO-2. He also sent UCO-2 a video that depicted a man masturbating. These image and video files did not include the man’s face.
 - i. Based on my training and experience, I believe that these image and video files are obscene.
- g. “Sean” also sent UCO-2 another picture that purportedly depicted himself. This image included the man’s face.

- i. Based on comparing these approximately four photographs to PORTER's current Ohio driver's license photograph, it appears that PORTER is the individual depicted in the four photographs sent by "Sean" to UCO-1.
- h. "Sean" suggested that he and UCO-2 communicate instead via text messages, and he provided his cellular telephone number to UCO-2 – that being 937-568-5895.
- i. Below are excerpts from the Meet24 chats summarized above:

Sean: hello beautiful my daughter is 12 and we have sex
 Sean: would you like to talk to my daughter
 Sean: I have sex with my daughter
 UCO-2: great
 UCO-2: y tell me that?
 Sean: to get you to talk to me
 Sean: is it ok I have sex with her
 UCO-2: i don't care
 Sean: do you want to talk to her
 UCO-2: y?
 Sean: well you're 13 and she's 12 I thought maybe you would want to talk to her why do you come on here
 UCO-2: let me see her
 Sean: *Sends image of a female child wearing clothing*
 Sean: her name is Jennifer
 UCO-2: yeah rite thats a screenshot from this app
 Sean: so why do you come on here
 UCO-2: so thats really not ur daughter rite?
 Sean: no that's not her
 Sean: I really don't have a daughter
 UCO-2: lol
 Sean: at least I got you to talk to me
 Sean: I've tried messaging you a dozen times with no reply
 UCO-2: says u live in like ohio rite?
 Sean: that's what it says but I really live in Kentucky

 Sean: are you really only 13
 UCO-2: yes im 13

 UCO-2: why is a pretty girl like you single I bet you got all kinds of guys trying to go out with you though
 UCO-2: well maybe u have heard there a pandemic and im in virtual school so hard to meet people
 Sean: you're quite feisty for thirteen

Sean: I like that in you
UCO-2: lol
Sean: so are you still a virgin
UCO-2: yes
Sean: well that's good
Sean: have you thought about sex before
UCO-2: yeah all the time
Sean: do you want to have sex soon
Sean: when did you start thinking about it all the time
UCO-2: yes i think so
UCO-2: i dunno the last few months
Sean: do you masturbate a lot
Sean: guess you don't want to tell me that lol
UCO-2: not a lot just sometimes
UCO-2: not a lot but sometimes
Sean: do you like it
Sean: when did you start masturbating I started when I was 13 too
UCO-2: how old r u really cause u aint 20 lol
Sean: no I'm 47
Sean: have you ever thought about being with an older man
UCO-2: ok cool
UCO-2: yes
Sean: so you don't mind my age then
UCO-2: no i don't care bout age
Sean: well that's nice can we be friends
Sean: who knows maybe something beautiful can happen
UCO-2: yea
UCO-2: like what
Sean: oh I don't know we just met each other
UCO-2: ok
Sean: do you have another picture of you
UCO-2: yes
Sean: *Sends image depicting a male who appears to be PORTER*
UCO-2: *Sends image of a female wearing clothing*
Sean: you are very pretty
Sean: so do your parents know you come here to this site
UCO-2: nope
.....
Sean: have you ever thought about having sex with an older man while
you masturbate
UCO-2: umm yeah i guess
Sean: well I thought about girls your age when I do it
Sean: talking to you turns me on to
.....
Sean: when was the last time you masturbated

UCO-2: i dunno couple nights ago
Sean: I did this morning
UCO-2: ok
Sean: was thinking about you
.....
Sean: would you like to meet me someday
UCO-2: u mean in person?
Sean: yes
UCO-2: maybe i dunno
UCO-2: could be fun
Sean: it would be a lot of fun I think
Sean: you said you haven't had sex before right
UCO-2: im a virgin yeah
Sean: *Sends close-up image of a male's penis*
Sean: would you like to have that
UCO-2: maybe
Sean: I would love to go down and lick you
Sean: I'll bet you taste so sweet
UCO-2: nobody ever done that to me
Sean: I know you would love it
UCO-2: probably lol
UCO-2: i heard its amazing
Sean: any chance I can see a picture of it
UCO-2: pic of what?
Sean: I've been told that I lick p**** better than a lesbian
Sean: a pic of your vagina
UCO-2: lol
UCO-2: sorry i don't have any pics like that on my phone
Sean: can't you take a picture
UCO-2: i mean i could texhnically yes
Sean: I'll do something for you
UCO-2: wht?
Sean: *Sends video depicting a male masturbating*
.....
Sean: I would love just to lay with you and cuddle and kiss and caress
each other
UCO-2: sorry just gotta be real careful right now my best friend got busted
for sending nudes to her boyfriend and his parents found them. she
is 13 also it turned into this huge ordeal ya know
Sean: I understand
Sean: well someday you'll be able to I can promise you I'm not a cop
.....
Sean: where else could you chat at
UCO-2: i really hust have this and texting
Sean: do you want my phone number

UCO-2: sure
Sean: 9375685895

87. After “Sean” provided his telephone number (that being 937-568-5895) to UCO-2 in the above detailed Meet24 communications, they communicated with each other via text messages. These communications transpired during the approximate time period of February 14, 2021 through February 15, 2021. Below is a summary of the text messages:

- a. UCO-2 reiterated that she was 13 years old, and “Sean” reiterated that he was 47 years old. “Sean” asked how UCO-2’s mother would react if she found out that UCO-2 was having a relationship with an older man.
- b. “Sean” and UCO-2 talked about what they would want to do if they met with each other in person. “Sean” said that he would want to have sex with UCO-2 in a hotel room.
- c. Below are excerpts from the text messages summarized above:

UCO-2: I told u I’m really 13 years old rite?
Sean: Yes you did tell me that
Sean: And I told you that I’m 47 right
UCO-2: Ok just wanted to make sure I don’t care bout age do u?
Sean: Is your mom strict or is she relatively easy with you
Sean: I don’t care about age either
UCO-2: She is pretty easy I guess
Sean: How would she react if she found out you were seeing an older man
UCO-2: Probably not good lol
Sean: Do you like the idea of being with me
UCO-2: Maybe I don’t know u that well yet
Sean: Well if we were to meet what would you want to do
Sean: And it doesn’t have to be sexual
UCO-2: What would u hope to happen? Just be honest and I’ll be honest if I’m ok with it
Sean: Well I would like to take you out to dinner and take you shopping and buy you some nice things
Sean: And then I would like to take you back to the hotel room and make sweet love to you
UCO-2: Ok lol
UCO-2: Sounds like ur nice
Sean: I wouldn’t hurt you sweetheart and if you didn’t want to make love I wouldn’t force you to do it
.....

Sean: Just so you know I deleted that other app I only want to talk to you
and I don't care about any other girls
Sean: There's no need for me to be there anymore so you're going to
have to talk to me is

Results of Subpoenas

88. On or around February 23, 2021 and March 16, 2021, two administrative subpoenas were served upon Wildec LLC requesting subscriber information and IP logs for any Meet24, FastMeet, Meet4U, and MeetEZ accounts associated with the following identifiers: "Sean", age 20, from Moraine, Ohio; and "Mike", age 20, from Moraine, Ohio. Records provided by Wildec LLC in response to the subpoenas provided the following information:
- a. An account containing the user identification number of **45521409** was created on or around October 6, 2020. The profile name for the account was "Sean", and the email address associated with the account was **sean2598@gmail.com**. The user's birthday was listed as October 6, 2000, his gender was listed as male, and his location was listed as Moraine, Ohio. The log of IP addresses identified that the account was logged into on approximately 119 occasions during the approximate time period of October 6, 2020 through October 15, 2020. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications) was utilized to log into the account on approximately 114 of these occasions. IP addresses serviced by the Verizon cellular telephone network were utilized to log into the account on the remaining approximately five occasions.
 - b. An account containing the user identification number of **45675752** was created on or around October 15, 2020. The profile name for the account was "Sean", and the email address associated with the account was **portersean68@gmail.com**. The user's birthday was listed as October 15, 2000, his gender was listed as male, and his location was listed as Moraine, Ohio. The log of IP addresses identified that the account was logged into on approximately 137 occasions during the approximate time period of October 15, 2020 through October 20, 2020. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications, the same IP address utilized to access the account detailed above) was utilized to log into the account on approximately 101 of these occasions. IP addresses serviced by the Verizon cellular telephone network were utilized to log into the account on the remaining approximately 36 occasions.
 - c. An account containing the user identification number of **45766959** was created on or around October 20, 2020. The profile name for the account was "Sean", and the email address associated with the account was **portersean68@gmail.com**. The user's birthday was listed as October 20, 2000, his gender was listed as male, and his location was listed as Moraine, Ohio. The log of IP addresses identified

that the account was logged into on approximately 74 occasions during the approximate time period of October 20, 2020 through October 24, 2020. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications, the same IP address utilized to access the accounts detailed above) was utilized to log into the account on approximately 49 of these occasions. IP addresses serviced by the Verizon cellular telephone network were utilized to log into the account on the remaining approximately 25 occasions.

- d. An account containing the user identification number of **45834215** was created on or around October 25, 2020. The profile name for the account was “Sean”, and the email address associated with the account was **portersean68@gmail.com**. The user’s birthday was listed as October 25, 2000, his gender was listed as male, and his location was listed as Moraine, Ohio. The log of IP addresses identified that the account was logged into on approximately 10 occasions on or around October 25. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications, the same IP address utilized to access the accounts detailed above) was utilized to log into the account on approximately eight of these occasions. IP addresses serviced by the Verizon cellular telephone network were utilized to log into the account on the remaining approximately two occasions.
- e. An account containing the user identification number of **45868159** was created on or around October 27, 2020. The profile name for the account was “Sean”, and the email address associated with the account was **portersean68@gmail.com**. The user’s birthday was listed as October 27, 2000, his gender was listed as male, and his location was listed as Moraine, Ohio. The log of IP addresses identified that the account was logged into on approximately one occasion on or around October 27, 2020. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications, the same IP address utilized to access the accounts detailed above) was utilized to log into the account on that date.
- f. An account containing the user identification number of **45887212** was created on or around October 28, 2020. The profile name for the account was “Mike”, and the email address associated with the account was **portersean68@gmail.com**. The user’s birthday was listed as October 28, 2000, his gender was listed as male, and his location was listed as Moraine, Ohio. The log of IP addresses identified that the account was logged into on approximately 891 occasions during the approximate time period of October 28, 2020 through December 8, 2020. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications, the same IP address utilized to access the accounts detailed above) was utilized to log into the account on approximately 734 of these occasions. IP addresses serviced by the Verizon cellular telephone network were utilized to log into the account on the remaining approximately 157 occasions.

- g. An account containing the user identification number of **47432599** was created on or around January 24, 2021. The profile name for the account was “Sean”, and the email address associated with the account was **portersean68@gmail.com**. The user’s birthday was listed as January 24, 2001, his gender was listed as male, and his location was listed as Moraine, Ohio. The log of IP addresses identified that the account was logged into on approximately 242 occasions during the approximate time period of January 24, 2021 through February 14, 2021. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications, the same IP address utilized to access the accounts detailed above) was utilized to log into the account on approximately 222 of these occasions. IP addresses serviced by the Verizon cellular telephone network were utilized to log into the account on the remaining approximately 20 occasions.

89. I noted the following information regarding the records detailed above from Wildec LLC:

- a. The IP address of 74.136.165.234 (an IP address serviced by Charter Communications) was utilized to access all seven of the accounts. The same two email addresses (**sean2598@gmail.com** and **portersean68@gmail.com**) were associated with the seven accounts. Based on this and other information detailed in the Affidavit, it is reasonable to believe that the same person utilized all seven accounts.
- b. The only IP addresses utilized to access the seven accounts were an IP address serviced by Charter Communications (74.136.165.234) and IP addresses serviced by the Verizon cellular telephone network. Based on my training and experience, I know that the use of IP addresses serviced by Charter Communications is consistent with someone using wireless Internet service at a residential or business location to access the Internet. I also know that the use of IP addresses serviced by Verizon is consistent with someone using the data plan from his/her cellular telephone to access the Internet.
- c. A different birthday was listed for each of the seven accounts. I noted that each of the birthdays used the same months and days of the months as the dates that the accounts were registered, with the year being 2000 for the first six accounts (which were registered in 2020) and 2001 for the last account (which was registered in 2021) – therefore purportedly making the user 20 years old, with his birthday being the same dates as the dates that the accounts were registered.
 - i. Based on my training and experience, I know that individuals who utilize electronic accounts in furtherance of their criminal activities often use fictitious identifying information (such as names and birthdays) when registering their accounts as a means to conceal their identities from law enforcement officers.

- ii. Based on the trend of the birthdays and other information detailed in the Affidavit, it is reasonable to believe that the account user was using fictitious birthdays when registering his Wildec LLC accounts.
90. On or around February 25, 2021, an administrative subpoena was served upon Charter Communications requesting subscriber information for the IP address of 74.136.165.234 (the IP address utilized to access the seven Wildec LLC accounts detailed above) on a sample of four of the dates and times that it was utilized to access the one of the “Sean” accounts (the account with the user identification number of **47432599**). Records received from Charter Communications in response to the subpoena identified that this IP address was subscribed to PORTER at the SUBJECT PREMISES. The records identified that this IP address had been leased to PORTER’s account during the approximate time period of September 27, 2019 through March 4, 2021 (the date that Charter Communications produced the records in response to the subpoena).
91. On or around March 16, 2021, an administrative subpoena was served upon WhatsApp requesting subscriber information associated with the WhatsApp account associated with telephone number 937-626-4691 (the telephone number that PORTER has used to communicate with PO Owens). Records received in response to the subpoena identified that there was a WhatsApp account associated with this telephone number. The only subscriber information available for the account was the model number for the device utilized to access the account – that being an Android device with a model of DIGILAND DL1023.
- a. Based on Internet research, I have determined that a DIGILAND DL1023 Android device is a tablet.
 - b. As detailed above, PO Owens has only authorized PORTER to utilize a flip-style cellular telephone and a Samsung tablet. PO Owens has not reviewed or monitored any other electronic devices.
 - c. Based on my training and experience, I know that individuals who are involved in child exploitation offenses and who are on probation or parole often conceal the devices that they use in furtherance of their criminal activities from their probation or parole officers. Such individuals often utilize multiple devices – one or more devices that they report to their probation or parole officers (which may be searched pursuant to the terms of their supervision) and other devices that they do not report (which they use for their child exploitation activities).

Identification of Additional Accounts

92. On or around March 16 and 18, 2021, FBI investigators reviewed publicly available information on various social media websites and messenger applications for any possible accounts associated with the email addresses **stphs141963@gmail.com**,

sean2598@gmail.com, and **portersean68@gmail.com** and telephone numbers 937-626-4691 (the telephone number that PORTER has used to communicate with PO Owens) and 937-568-5895 (the telephone number that “Sean” used to communicate with UCO-2). Among other accounts, the investigators located the following:

- a. A WhatsApp account was located that was associated with telephone number 937-626-4691. The profile picture for the account depicted a white male who appears to be PORTER. The WhatsApp profile picture appears to be the same profile picture for the “Sean” Wildec LLC account that was used to communicate with UCO-2.
- b. A Snapchat account was located that was associated with telephone number 937-626-4691. The account had a user name of **sporter4020** and a profile or display name of “Sean Porter”.
- c. A Skype account was located that was associated with telephone number 937-626-4691. The account contained a user name of **live:.cid.58d10c2422ccf850** and a profile or display name of “sean dobbins”. The profile picture for the account depicted a white male who appears to be PORTER.
- d. Another Skype account was located that was associated with the email address **stphs141963@gmail.com**. The account contained a user name of **live:stphs141963** and a profile or display name of “Sean Porter”.

Conclusion Regarding Use of Accounts

93. Based on the information detailed above, there is probable cause to believe that PORTER is the user of the “Sean” and “Mike” Wildec LLC accounts that were utilized to communicate with UCO-1 and UCO-2. There is also probable cause to believe that PORTER is the user of the following accounts:
 - a. The Google accounts associated with the email addresses **stphs141963@gmail.com**, **sean2598@gmail.com**, and **portersean68@gmail.com**;
 - b. The Meet24, FastMeet, Meet4U, and/or MeetEZ accounts containing the user identification numbers of **45521409**, **45675752**, **45766959**, **45834215**, **45868159**, **45887212**, and **47432599** and/or associated with the email addresses **sean2598@gmail.com** and **portersean68@gmail.com**;
 - c. The Skype accounts containing the user names of **live:.cid.58d10c2422ccf850** and **live:stphs141963**;

- d. The Snapchat account containing the user name of **sporter4020**; and
- e. The WhatsApp accounts associated with telephone number 937-626-4691.

94. Also based on the information detailed above, there is probable cause to believe that PORTER has utilized at least two of his Meet24 accounts and a mobile device to (1) attempt to coerce and entice minors to produce and send him child pornography; (2) to attempt to receive and possess child pornography; (3) to attempt to transfer obscene materials to minors; and (4) to attempt to persuade, induce, entice, or coerce a purported minor to engage in criminal sexual activity.

Evidence Available in Email, Social Media, and Messaging Accounts

95. In my experience, individuals often post information on their social media accounts, dating websites, and messaging accounts (such as Skype, WhatsApp, Snapchat, and Google Messaging) about other electronic accounts that they utilize – including their email addresses, other social media accounts, and messenger accounts. This information may provide evidentiary value to child exploitation investigations in that it may help in identifying other accounts utilized by the offenders in furtherance of their child exploitation activities.
96. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, dating websites, and messaging accounts (such as Skype, WhatsApp, Snapchat, and Google Messaging). I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
97. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media accounts, dating websites, and messaging accounts (such as Skype, WhatsApp, Snapchat, and Google Messaging) as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
98. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, photo sharing services (such as Google Photos), social media accounts, dating websites, and messaging accounts (such as Skype, WhatsApp, Snapchat, and Google Messaging). Individuals also often attempt to obtain child pornography from

a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

99. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims. Based on the records obtained by Wildec LLC, it appears that PORTER has utilized various aliases and false identities.
100. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.
101. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child pornography and child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.
102. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.
103. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations.

This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

104. Google Contacts provides users with address books to store their contacts. Based on my training and experience, I know that individuals involved in child pornography offenses often store contact information for their co-conspirators and their victims in their contact lists. This information can be materially relevant to identifying the co-conspirators and victims.
105. Google Calendar provides users with appointment books. In my training and experience, individuals involved in child pornography offenses may store information in their appointment books about meetings with their victims.
106. Google's Chrome and My Activity service stores information about Internet searches conducted by its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.
107. Google Drive, Google Keep, and Google Photos provide users with cloud computing and online file storage. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full and/or as a means to back up their files. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.
108. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.
109. As detailed above, Google Location History is an application in which Google utilizes various data such as cell site information and Wi-Fi routers to locate and geo-locate a cellular telephone device. Google collects and stores this data if the application is enabled by the user, either during the set-up of the device or through the device's settings. Also as detailed above, Google Maps stores information about maps and directions searched for on Google's search engine.
110. Based on my training and experience, I know that location information from cellular telephones and Google accounts, as well as maps and directions searched for on the Google search engine, can be materially relevant in investigations involving child exploitation offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims. Data regarding the subjects'

whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place. Furthermore, data regarding the subjects' whereabouts as obtained from the location information can lead to the identification of the places where computer devices used in furtherance of the crime may be present.

Conclusion Regarding Probable Cause

111. Based on all of the information detailed above, there is probable cause to believe that information associated with the following accounts may contain evidence of PORTER's child pornography and child exploitation offenses:
- a. The Google accounts associated with the email addresses **stphs141963@gmail.com**, **sean2598@gmail.com**, and **portersean68@gmail.com**;
 - b. The Meet24, FastMeet, Meet4U, and/or MeetEZ accounts containing the user identification numbers of **45521409**, **45675752**, **45766959**, **45834215**, **45868159**, **45887212**, and **47432599** and/or associated with the email addresses **sean2598@gmail.com** and **portersean68@gmail.com**;
 - c. The Skype accounts containing the user names of **live:.cid.58d10c2422ccf850** and **live:stphs141963**; and
 - d. The Snapchat account containing the user name of **spporter4020**.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

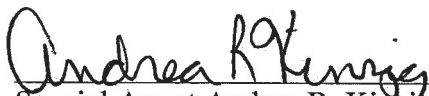
112. I anticipate executing the requested warrants for the listed accounts under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Google LLC, Wildec LLC, Microsoft Corporation, and Snap Inc. to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 through B-4. Upon receipt of the information described in Section I of Attachments B-1 through B-4, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-4.

CONCLUSION

113. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; including violations of 18 U.S.C. §§

2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(1), 2252(a)(2) and (b)(1), 2252A(a)(2) and (b)(1), 18 U.S.C. §§ 2252(a) and (e), 18 U.S.C. § 2422(b), and 18 U.S.C. § 1470, are present in the information associated with the above noted accounts (as described in Attachments A-1 through A-4).

114. I therefore respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-4.
115. Because the warrants for the accounts described in Attachments A-1 through A-4 will be served on Google LLC, Wildec LLC, Microsoft Corporation, and Snap Inc., who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 30th of March 2021


Sharon L. Ovington
United States Magistrate Judge

